COMBINED FEDERATED BATTLE LABORATORIES NETWORK (CFBLNet)

PUBLICATION 1
ANNEX D

NETWORK OPERATIONS
(Network/System Aspects of CFBLNet)

Version 5.0
December 2007

DOCUMENT CONTROL AND TRACKING METADATA

Security Classification	Unclassified
Access Status	Version 5.0
Usage Condition	Publicly Releasable

Scheme Type	CFBLNet Documentation Control and Tracking Scheme
Scheme Name	See Pub 1, Annex E, Appendix 2 – CFBLNet Version Labelling
Title Words	CFBLNet Pub 1 – Annex D, CFBLNet Network Operations (Network/System Aspects of CFBLNet)

Function Descriptor	Network Operations
Activity Descriptor	Informational

Event Date	Agent Type	Agent Name	Agent Details	Event Type	Event Description
13 Dec 07	C-EG	Charles Tulaney	C-EG Chair	Review/Approve Sign	Publication 1, Version 5.0

TABLE OF CONTENTS

*__ADDITIONAL APPENDICES__

__APPENDIX 1 – CFBLNet LEVEL 0 TOPOLOGY (UNABRIDGED)__

__APPENDIX 2 – BLACK IP ADDRESS SPACE ALLOCATION__

__APPENDIX 3 – CFBLNet VOIP PHONE NUMBER RANGES__

** Note: Additional Appendices are contained in a separate document.*

CHAPTER 1 – INTRODUCTION

Purpose

101. Annex D to the CFBLNet Publication 1 (Pub 1) contains the network operations and system management policies and procedures, related to the operations of the CFBLNet, which functions under the authority of the CFBLNet Technical Arrangement (Charter). It comprises a main body and a range of appendices. Appendices that may not be visible have been deemed to be of a sensitive nature and are available only in a controlled version.

Authority

102. Annex D is issued by the CFBLNet Executive Group (C-EG) on behalf of the CFBLNet Senior Steering Group (C-SSG). The provisions of this and all associated publications shall govern the conduct of all network activities performed by the CFBLNet participants, subject to their respective Nation's laws and military regulations.

103. The Network Working Group (NWG) is the technical body, comprised of appropriate experts from the Charter Nations/Organizations (CN/Os), which supports the network governance process for the CFBLNet on behalf of the C-EG. The terms of reference and responsibilities of the NWG are described within Annex A.

Amendments

104. Pub. 1 Annex D may be amended when the NWG determines that there is an identified requirement. The NWG Chairman will propose the text of the amendment to the NWG members for endorsement. Once the NWG members have endorsed the amendment, it will be submitted for C-EG approval. Upon approval by the C-EG, the Secretariat will re-issue a new version of Annex D.

Effective Date

105. The current version of CFBLNet Pub 1, Annex D is effective upon the latest approval by the C-EG.

CHAPTER 2 – NETWORK OVERVIEW DESCRIPTION

Infrastructure

201. The CFBLNet infrastructure is a closed, wide area communications network linking CN/Os' infrastructures, collectively forming the CFBLNet. The CFBLNet Level 0 Topology is illustrated in Appendix 1 of this document. The NWG representatives are responsible for maintaining the individual CN/O Level 1 and Level 2 topology diagrams with the requisite detailed information.

202. The CFBLNet consists of the following components:

a. Black backbone (BLACKBONE). A common, closed, unclassified IPv4/v6 routed network layer implemented using a mixture of both ATM and IP bearer networks. Its primary purpose is to transport encrypted traffic throughout the network. The level and type of network services available within this component will be the minimal required to support the interconnection of multiple enclaves as agreed to by all CN/Os; see Chapter 5, Table D-5.1 of this document.

b. CFBLNet Unclassified Enclave (CUE). A permanent IPv4/v6 enclave operating over the BLACKBONE and for a period of time over legacy ATM and IP bearer network infrastructures. It will operate at the Unclassified, Non Releasable to Internet releasable to CN/Os and to Sponsored Nations/Organizations (SN/Os) as directed by the C-EG.

c. BLUE Enclave. A permanent classified IPv4 routed logical network operating over the BLACKBONE and for a period of time over legacy ATM and IP bearer network infrastructures. It operates as a System High logical network at the SECRET level, releasable AUSCANNZUKUS + NATO. An agreed level and implementation of network services within this enclave will be supported by the NWG in light of anticipated activities; and

d. Active and Inactive Enclaves. Active enclaves are created for a finite period to support the execution of specific Initiatives and operate over the BLACKBONE and for a period of time over legacy ATM and IP bearer network infrastructures. Specific enclaves may become inactive based upon respective Initiatives event schedule. The level of classification and release caveats used within these enclaves will be determined by the Initiative requirements. The coordination and provision of all network services within a specific temporary enclave will be the responsibility of the Initiative Sponsor.

203. Operational control of all CN/O network devices must conform to the CFBLNet Pub 1 requirements. CN/Os are responsible for providing connectivity between their national sites and an agreed upon national/organizational Point Of Presence (POP) which will serve as their connection point to the CFBLNet. See paragraph 206.

204. Initiative Participants can establish connectivity via any accredited means in accordance with Pub 1 Annex C, such as ISDN dial-up or dedicated leased lines.

CFBLNet Sites

205. CFBLNet sites are those operational participant sites accredited through the CFBLNet security process (Pub 1 Annex C) and approved by the C-EG-. Each NWG member will confirm their list of new/existing sites and site numbers as assigned by CFBLNet Secretariat at each CMM. This list does not need to include individual CN/Os' Initiative sites as this is the CN/O's prerogative. The NWG is not part of the site approval process.

206. **National/Organizational Point Of Presence.** A CFBLNet national/organizational POP is a CFBLNet site that provides a point of connectivity between different national/organizational management and administrative domains. The establishment of a peering relationship between two national/organizational POPs is done with the consent of the CN/Os involved.

Cryptographic Services

207. **Cryptographic Support.** The Multinational Information Sharing Program Management Office (MNIS PMO) is responsible for the coordination of cryptographic services for the permanent components of the CFBLNet from the USA sites to national/organizational POP sites. Behind a CN/O's POP, that CN/O will be responsible for coordinating their cryptographic services and will provide this information to the NWG. Each CN/O may provide their own cryptographic support for their respective information and administrative domains or arrange other support accordingly. Initiative Sponsors that require special cryptographic services are to coordinate support through their respective CLR.

208. **Encryption Devices.** CFBLNet enclaves are protected by appropriate and approved encryption devices and border protection systems (BPS) accredited by CN/Os for the protection, as required, of information up to and including the classification level of SECRET.

209. **Keying Material (Keymat).** The MNIS PMO typically serves as the controlling authority for the Keymat (DS101 and DS74) implemented by the CN/O's designated communications security (COMSEC) authorities. This will typically be the case for all international links from one national/organizational POP to another. CN/Os can utilise their own national or regional (NATO) key between their own internal/national sites if they so choose. An Initiative Sponsor may choose to coordinate Keymat implementation with other controlling authorities provided the implementation is in accordance with all associated CN/Os policies and regulations. If required, a COMSEC CALL OUT Message will be sent out via secure message traffic by the responsible Keymat COMSEC Custodian addressed to Initiative Participants. The COMSEC CALL OUT MESSAGE will include special instructions: Keymat short title, valid dates, and participants at a minimal.

CHAPTER 3 – MANAGEMENT ASPECTS

Introduction

301. This chapter addresses the management requirements of the CFBLNet and is intended to provide a basic understanding of the network operations and the relationship between the CN/Os' management cells.

Management Strategy

302. Each CFBLNet CN/O provides, manages, supports and is responsible for their infrastructure, which collectively forms the CFBLNet. The USA Combined Communications Control Centre (CCCC) is recognised by the CN/Os as the central body responsible for coordinating the CFBLNet management policies as defined in this Annex.

303. The CFBLNet is currently a 24x7-accessible network. The CCCC located at the MNIS PMO in Arlington, Virginia, USA is staffed appropriately to support this effort. Initiative Participant manning is based on the requirements dictated by approved CFBLNet Initiatives.

MNIS PMO

304. The MNIS PMO operates and maintains the CCCC and provides the CFBLNet Secretariat resources that coordinate the use of the CFBLNet for Initiatives. The MNIS PMO is responsible for all POP connections within and to the USA WAN infrastructure. The CCCC manages and monitors CFBLNet activities and makes any pertinent information available to the CN/Os during normal operating hours (16x5). The CCCC will provide extended support as required for a specific Initiative as defined in the Memorandum of Agreement/Service Level Agreement (MOA/SLA).

NATO C3 Agency

305. The NC3A operates and maintains the European regional POP for NATO nations, NATO organizations and sponsored nations/organizations and also provides the cryptographic bridging between NATO, CCEB and USA environments and sponsored nations and organizations.

306. The NC3A also provides minimal regional NATO nation Secretariat for NATO and sponsored nations.

Incident Management

307. The CN/Os are responsible to advise the CFBLNet Secretariat of any CFBLNet activity that is not in compliance with CFBLNet policies and practices. Incidents reported to the CFBLNet Secretariat will be resolved through dialogue with the CN/Os involved. If the situation cannot be resolved, then recommendations will be made to the C-EG for resolution.

Network Documentation

308. Each CN/O will maintain their own detailed network documentation and will make it available as required by the other CN/Os.

309. There are three levels of documentation that will comply with the security classification appendix within Pub 1 Annex C and are not intended to conflict with CN/O information security/disclosure policies:

a. Level 0. Basic CFBLNet WAN layout drawings showing major components and generic architecture at a level detailing the national Participants and the connectivity attributes between them. (Section 1: Intra-national topology; Section 2: Enclave topology; Section 3: Cryptographic topology; Section 4: BLACKBONE architecture);

b. Level 1. Detailed C/NO layout drawings, showing major components and generic architecture within a CN/O's domain (Section 1: Topology diagram; Section 2: Enclave matrix; Section 3: Cryptographic plan per site/enclave; Section 4: BLACKBONE); and

c. Level 2. Detailed CN/O site layout drawings, showing IP Addresses, Host Names, cards/ports, hardware/software, versions/revisions, etc. *

** Each nation may share details with relevant countries according to national security standards.*

Documentation Guidelines

310. Visio or MS PowerPoint are the preferred documentation tools. Where possible, documentation should be distributed to the NWG with the capability to drill down to network information where appropriate.

CHAPTER 4 – NETWORK SERVICES OVERVIEW

General

401. Each CN/O maintains and operates agreed levels and types of network services for the CFBLNet permanent components in order to facilitate Initiatives. These network services inter-operate with other CN/Os' services to provide a collective network community. The operation of permanent network services will be coordinated by the CCCC with each CN/Os designated Network Operations Centre (NOC).

Core Network Services

402. Core network services are robust, reliable and stable services, which have been developed and deployed on the CFBLNet permanent components to support Initiatives. They are managed and supported directly by the CN/Os. They are further divided into the following two categories:

a. Critical Infrastructure. Those services that each CN/O is obligated to stand up and support, as part of their minimum network infrastructure, for effective and efficient network operations; and
b. Supporting Infrastructure. Those services that provide a value added benefit but which are not essential for effective network operations and can be hosted by any CN/O on behalf of other CN/Os.

403. The NWG provides recommendations to the EG on what core network services will be deployed on the CFBLNet permanent components, its category and operational status in light of anticipated activities. It is the responsibility of the Initiative Sponsors to determine and support any network services that are required within a temporary enclave, as these will be deemed separate from the CFBLNet Core Network Services.

404. An Initiative may deploy additional network services required to support activities specific to that Initiative. As part of the review of Initiative activities, the NWG will consider these additional network services for inclusion as part of the CFBLNet core network services for some or all of the CFBLNet permanent components. This process is managed by the NWG and follows the method illustrated in Figure D-4.1.

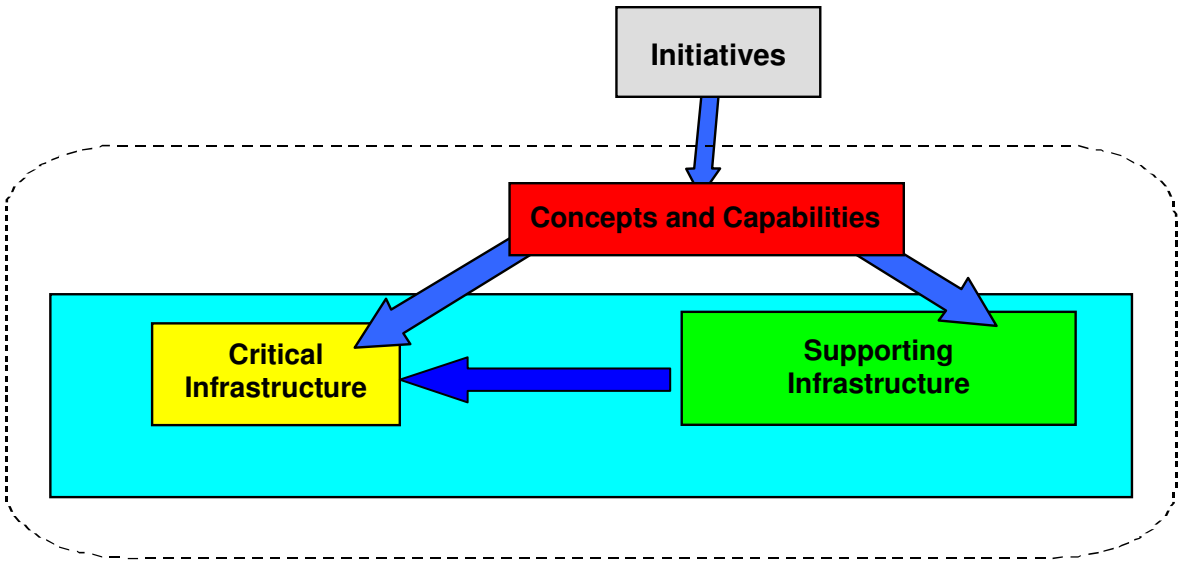


Figure D-4.1, CFBLNet Network Services

Internet Protocol (IP) Address Space

405. CN/Os are responsible for managing their own IP address space to support their network infrastructure requirements. IP address spaces are allocated through the NWG.

406. CN/Os will use an agreed upon IP address space for the CFBLNet permanent components (detailed in Appendix 2), thus minimizing the possibility of address space conflict. The CCCC is responsible for maintaining a register of all CFBLNet IP address spaces.

407. CFBLNet Initiatives, utilizing the permanent components, will coordinate with their respective NWG representative to obtain IP space allocations. For those Initiatives utilizing a separate temporary enclave, NWG representatives will recommend the IP address space allocation for use within the enclave.

408. The CCCC is responsible for the assignment of Border Gateway Protocol (BGP) Autonomous System (AS) numbers to each CN/O.

CHAPTER 5 – CFBLNet BLACKBONE

General

501. The purpose of the BLACKBONE is to provide a permanent, common, closed, unclassified transport (bearer) layer. Its primary function is to transport encrypted traffic throughout the network. There are no network services available within this component (e.g., e-mail or VoIP) except those required to support the execution of multiple enclaves as agreed to by all CN/Os.

502. The core network services for the BLACKBONE are depicted in Table D-5.1.

Ser (a)	Information Service Description (b)	Status (c)
1	Internet Protocol Addressing	Required
2	Network Service Access Point Addressing	Required
3	Routing Protocols (e.g., OSPF, BGP4, IGP, EIGP)	Required
4	Network Time Protocol (NTP)	Required
5	Internet Protocol version 6 (IPv6)	Available
6	IP Multicasting	Available
7	Bandwidth Management	Available

Table D-5.1, IPv4 BLACKBONE Core Network Services

Routing Protocols

503. The primary routing protocol used on the CFBLNet BLACKBONE will be Border Gateway Protocol (BGP). Choice of routing protocol for CN/O internal distribution of routes will be at the discretion of each CN/O.

Network Management

504. The BLACKBONE network management tools implemented by the CCCC are the Joint Defense Information Infrastructure Control System-Deployed (JDIICS-D) based on HP OpenView, BMC Patrol, CISCO Works and Open-Source Ticket Request System (OTRS). In addition, each Participant may implement network management tools at their own discretion. Each CN/O must identify the router and switch interfaces that require management/monitoring to the CCCC. CN/Os will coordinate with the CCCC for use of SNMP community strings including password length, complexity and frequency of change.

CHAPTER 6 – BLUE ENCLAVE CORE NETWORK SERVICES

General

601. The BLUE Enclave is a permanent classified TCP/IP routed logical network operating over the BLACKBONE. It operates as a System High logical network at the SECRET level, releasable AUSCANNZUKUS + NATO.

602. The core network services for the BLUE enclave are listed in Table D-6.1.

Ser (a)	Information Service Description (b)	Status (c)
1	Domain Name Service (DNS)	Required
2	E-mail (SMTP)	Required
3	Web (HTTP)	Available
4	Network Time Protocol (NTP) Source	Required
5	IP Telephony Call Manager	Required
6	VOIP phone @ each site	Required

Table D-6.1, BLUE Enclave Core Network Services

Domain Name Service (DNS)

603. The BLUE enclave supports a distributed DNS service with each CN/O being responsible for managing its own DNS domains in accordance with IETF standards.

604. The BLUE enclave DNS is a federation of DNS servers, with the USA and GBR providing a dual '.' root master with other CN/Os and NATO assigned with a secondary '.' root. Each CN/O has the primary DNS responsibilities for their individual domain space.

Electronic Mail (e-mail)

605. The BLUE enclave supports a distributed e-mail service between CN/Os. E-mail is considered a critical infrastructure service.

606. Simple Message Transfer Protocol (SMTP) is the agreed e-mail protocol between CN/Os. CN/Os may implement their own national e-mail protocols, ensuring they provide an SMTP interface at their national/organizational POP boundary.

607. In general, e-mail on the BLUE enclave is routed according to the DNS Mail Exchange (MX) record. Other (e.g. static) mail routing can be implemented as agreed between CN/Os.

E-mail Account Naming Convention

608. Participant will establish e-mail accounts as either:

a. Permanent accounts for management or engineering purposes; or
b. Temporary accounts for each Initiative as required.

609. There are three types of accounts that can be used in the BLUE enclave to effect communications between users as listed in Table D-6.2.

Ser (a)	Account Type (b)	Example (c)
1	Personnel–normally used for enduring accounts (management, engineering etc)	bill.smith@, felicity.smith@
2	Organizational–normally used for operational/warfighter accounts	cflcc.g6@, asbde.s3@uk3cdobde.s2
3	Group–for address lists	CCCC.staff@, cflcc.staff@

Table D-6.2, BLUE Enclave E-mail Account Strategy

610. The recommended convention for BLUE enclave e-mail accounts is:

<first name>.<last name>

Web Services

611. The BLUE enclave supports the Web service (HTTP and HTTP/S) protocols to provide Web services across the BLUE enclave for management and engineering coordination as well as the delivery of Web-based information sources and products for Initiatives.

612. CN/Os are actively encouraged to populate these Web services in support of information dissemination for the purposes of CFBLNet management/coordination and to support Initiatives. CN/Os should advise the NWG when a permanent or temporary Website is established in the BLUE enclave.

613. The CFBLNet Secretariat has established the primary password-protected Internet Website for CFBLNet matters (http://www.disa.mil/cfblnet, www.cfblnet.info). This Web server will be the primary vehicle for disseminating information to the CFBLNet management community and will include unclassified publications, network and site diagrams, DNS tree structure, Initiative schedules, Initiative description and results. Should classified information need to be published, a Website will be stood up in the BLUE enclave.

Network Time Protocol (NTP)

614. The BLUE enclave supports the Network Time Protocol (NTP) in order to provide a stable time source, synchronized across the wide area.

615. A Stratum 1 time source located at NATO is the primary NTP source for the BLACKBONE and BLUE enclave. AUS, CAN, GBR, NATO and the MNIS PMO routers are peered with each other, recognizing the NATO router as a Stratum 2 time source. Other CN/Os will establish a one way server relationship with their nearest time source.

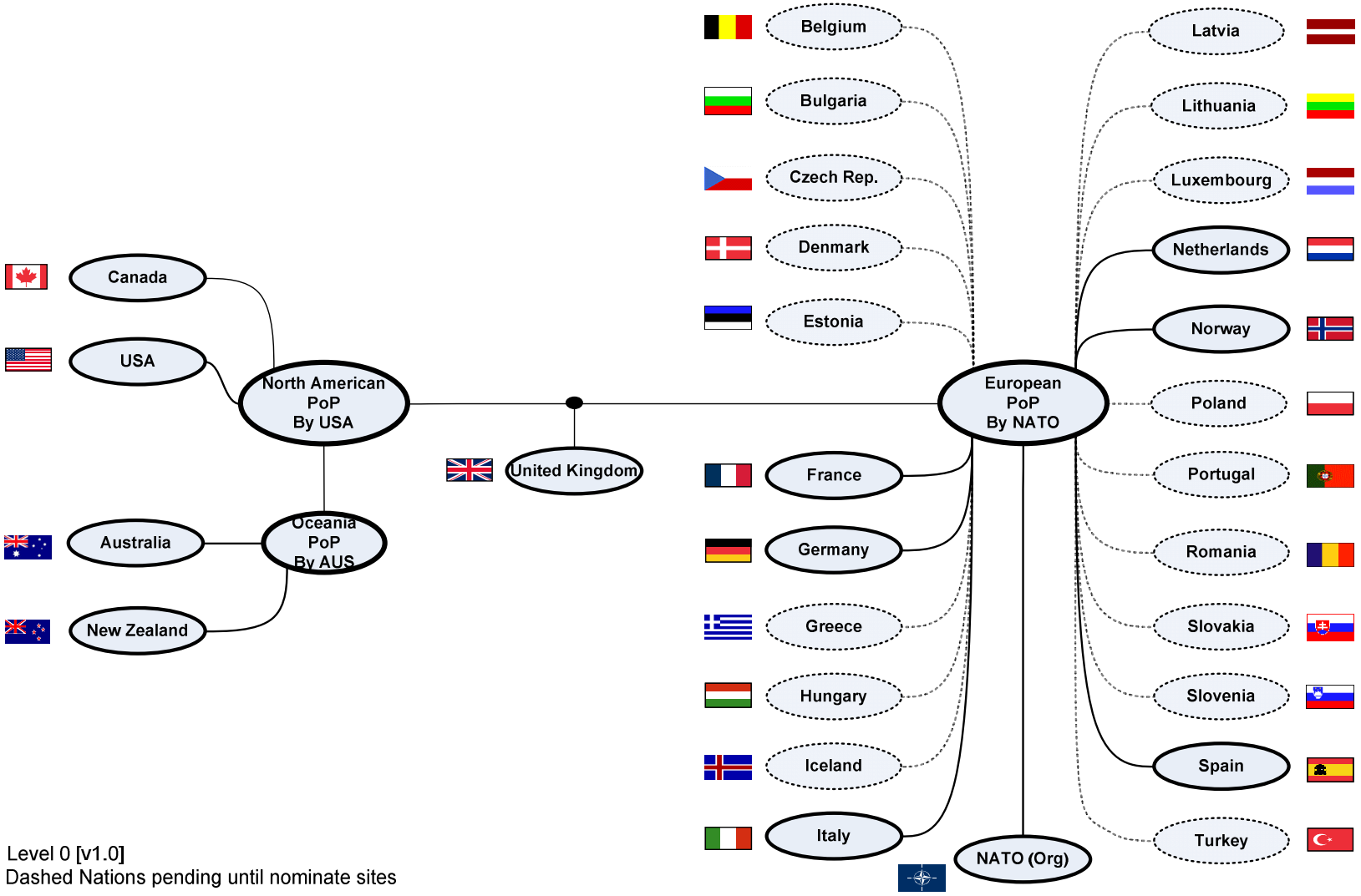
IP Telephony

616. The BLUE enclave supports IP Telephony (VoIP) for in-band secure communications between the CN/Os. It is also the primary means of secure communications for the CFBLNet management and engineering communities.

617. Each BLUE enclave site should have at least one VoIP (hardware or software phone) capability onsite as a minimum that is compatible with the BLUE enclave standard system. This phone is primarily for engineering management and coordination. Each site must coordinate with a “Call Manager-enabled” site to have its VoIP phone managed.

618. The Voice over IP (VoIP) Phone Numbers allocated for the BLUE enclave are detailed in Appendix 3 -- BLUE Enclave VoIP Phone Number Ranges and the NATO portal.

APPENDIX 1 – CFBLNet Level 0 Topology



Level 0 [v1.0]
Dashed Nations pending until nominate sites